Perspectivas de investigación

Autodeterminação informativa, inteligência de estado e o direito ao esquecimento na web: desafios contemporâneos aos profissionais da informação

Maria Aparecida Moura
Universidade Federal de Minas Gerais
Brasil · mamoura@ufmg.br

Resumo: O texto aborda os fundamentos normativos referentes à proteção dos dados pessoais e ao desenvolvimento da atividade de inteligência no Brasil no contexto da autodeterminação informativa e do direito ao esquecimento digital. Apresenta o núcleo comum das normativas sobre proteção de dados pessoais em nível internacional e os fundamentos da atividade de inteligência no Brasil. Analisa os desafios contemporâneos à formação de profissionais da informação para trabalhar com informações sensíveis no âmbito de atividades estratégicas tensionadas por mudanças culturais, legais e tecnológicas em relação à proteção dos dados pessoais.

Palavras-chave: Autodeterminação informativa; Atividade de inteligência; Direito ao esquecimento; Informação sensível.

Abstract: The text discusses the normative foundations relating to the protection of personal data and the development of intelligence activity in Brazil in the context of informational self-determination and the right to digital oblivion. It presents the common core of the regulations on personal data protection at the international level and the fundamentals of intelligence activity in Brazil. It Analyzes the current challenges to the training of information professionals to work with sensitive information within the strategic activities tensioned by cultural, legal and technological changes regarding the protection of personal data.

Keywords: Informational Self-Determination; Intelligence Activities; Right to be Forgotten; Sensitive Information.

1 Introdução

> "Os principais meios de obter segurança, ao que parece, são as novas técnicas e tecnologias de vigilância, que supostamente nos protegem, não dos perigos distintos, mas de riscos nebulosos e informes. As coisas mudaram tanto para os vigilantes quanto para os vigiados." (David Lyon)[1]

Nos últimos anos a Ciência da Informação tornou um campo científico de relevância estratégica, indo além dos elementos retóricos. Se, ao longo de décadas, o campo científico atuou na dinamização do fluxo do capital-informação por meio da implementação de procedimentos técnicos, o desafio contemporâneo e o de pensar as implicações sociais e tecnológicas da infraestrutura global da informação. Tal desafio ocorre em contextos econômicos e de Inteligência de Estado tensionados pelo uso desautorizado de informações sensíveis, como o que se observou no recente fato social envolvendo a Sony Pictures que colocou em disputa sócio-política os Estados Unidos e a Coréia do Norte. O referido fato teve como consequências e dínamos a subtração de informações industriais, o *blackout* no acesso Internet de um Estado Nacional e o fortalecimento de modelos de negócio focados na distribuição digital da informação. Essas mudanças no modelo global de produção e distribuição da informação implicam em a Ciência da Informação repensar-se como campo científico que atua estrategicamente na emergência do fenômeno informacional.

Um dos aspectos preocupantes nessa conjuntura, orientada pela conexão em rede, pelo tráfego intenso de informações monitoradas por *drones,* arquivos panópticos e pela "*Weltanschauung* da ubiquidade do perigo[2]", é exatamente a capacidade dos espaços formativos incorporarem criticamente essas novas demandas sociais.

Parece-nos que o campo da Ciência da Informação tem sido ostensivamente convocado a incorporar em sua dinâmica reflexiva e modelos formativos uma compreensão alargada dos riscos, desafios e oportunidades profissionais que essa pletora de mudanças anuncia.

Assim, no desenvolvimento desse trabalho tomaram-se por referência conceitos transversais que orientam a atual discussão referente à organização, processamento e difusão de informações sensíveis em interface com a necessária proteção dos dados pessoais no contexto brasileiro. Partiu-se do reconhecimento que, devido aos processos de difusão desordenada e inadvertida das informações pessoais por dispositivos de sociabilidade eletrônica, comércio eletrônico e serviços estatais de monitoramento em rede, tornou-se urgente a compreensão das dimensões sociais e políticas envolvidas na gestão profissional dessa massa de dados, tomando-se por referência a soberania nacional e a autodeterminação informativa dos cidadãos brasileiros.

2 Dimensão conceitual e técnica da proteção dos dados pessoais

O debate contemporâneo acerca dos processos do acesso e difusão de informações sensíveis oriundas de diferentes cidadãos e Estados Nacionais em âmbito global colocou a governança informacional e a vigilância panóptica como uma dimensão estruturante do mundo moderno. Compreender suas dimensões conceituais parece ser necessário à efetivação de análises críticas e atuação nesse cenário poroso do ponto de vista do fluxo, comércio e acesso à informação e aos dados pessoais em combinação com a dimensão sensível a eles referido.

A Razão de Estado é, conforme salienta FOUCAULT (2008: p.318) "o tipo de racionalidade que possibilitar manter e conservar o Estado a partir do momento em que ele é fundado, em seu funcionamento cotidiano, em sua gestão de todos os dias." A razão de Estado se articula em torno de dois conjuntos de tecnologias políticas: uma tecnologia diplomático-militar (busca de alianças, fortalecimento do exército) e a polícia (os meios necessários para fortalecer o Estado desde o interior). A razão do

[1] BAUMAN, Zygmunt. (2013) *Vigilância líquida*. Rio de Janeiro: Zahar.
[2] Idem.

Estado vincula-se à formação de saberes precisos capazes de garantir a permanência e o desenvolvimento do Estado.

A razão de Estado tem como instrumentos a guerra, que visa manter a manutenção do equilíbrio entre os Estados; a diplomacia, que visa às negociações e a articulação de informações sobre o poder em cada país; o dispositivo militar permanente, que objetiva o cálculo das relações diplomáticas, políticas e econômicas e o aparelho de informação,

> "que possibilita ao Estado o conhecimento das próprias forças e a ocultação destas aos olhos dos outros, bem como a obtenção de informaçõe*s* sobre o poder dos aliados e adversários, disfarçando possuí-las." SANTOS (2010: p.187).

A inteligência de Estado, que se orienta fundamentalmente pela obtenção do dado negado, se caracteriza como um órgão de assessoramento ao processo decisório e se estrutura em torno de três aspectos centrais: o produto, o processo e a organização. Os serviços de inteligência têm como marcas primordiais os grandes volumes de informação que precisam ser coletados, tratados e analisados para orienta estrategicamente os tomadores de decisão.

Todavia, conforme salienta GONÇALVES (2011: p. 110).

> "A grande discussão relacionada à atividade da inteligência em regimes democráticos continua se referindo à maneira como os serviços secretos devem atuar sem que violem as leis e princípios do Estado democrático de direito. Teme-se, também, o uso da inteligência com fins político-partidários por governos e, ainda, o excesso de poder dos órgãos de inteligência, por lidarem com informações sigilosas."

No contexto do acesso à informação, nota-se, no entanto, um conflito de interesses entre a razão de Estado e a proteção da intimidade e dos dados pessoais. Nota-se ainda que, a intermediação tecnológica e semântica ampliou a conexão e a inteligibilidade de inúmeras informações disponibilizadas livremente na web e que eram consideradas triviais em sua origem. Nesse sentido, naturalizam-se os dispositivos e rotinas de auto-exposição e de monitoramento internacional através de geolocalizadores, câmeras de monitoramento, dentre outros dispositivos de controle e conexão.

A informação sensível é aquela cujo comprometimento, a alteração, o roubo fraudulento ou a destruição pode prejudicar a continuidade do funcionamento dos serviços do estado e o exercício do poder em situação normal ou em situações de crise. Para proteger a informação é preciso conhecer e identificar a informação. São tarefas dos profissionais da informação nesse contexto: a identificação dos dados, a definição da sensibilidade das informações, a definição de políticas de compartilhamento e a definição de políticas de armazenamento.

A autodeterminação informacional é compreendida como o controle pessoal sobre certos aspectos da identidade projetada no mundo. Nesse sentido, refere-se ao direito de definir quem deve utilizar e propagar as informações que nos concernem. Todavia, a perspectiva de que a autodeterminação informativa na web encontra-se sob ameaça, vincula-se, sobretudo, à grande expansão e ao engendramento de arquivos panópticos que permitem a conexão dos dados pessoais a partir de diferentes técnicas e meios de arquivamento do ordinário.

O caráter difuso presente nos conceitos de dados pessoais, intimidade e propriedade intelectual tornou bastante fugidio a governança informacional em ambientes digitais. A perspectiva de qualidade da informação, dependente, nos dias atuais, da velocidade, diversidade e conexão digital entre documentos, dispostos originalmente em múltiplas fontes, pode sofrer alterações significativas decorrentes de questionamentos éticos advindos da conexão ostensiva e perene entre os produtos do espírito e as trajetórias humano-sociais.

De acordo com DROUARD apud AVERNA E BEAUFOND[3],

[3] AVERNA Louise, HUYGHUES-BEAUFOND Christelle. Le droit à l'oubli numérique. Accessible à l'adresse: http://www.e-juristes.org/le-droit-a-loubli-numerique/. Acesso em 28 jul 2014.

> "A problemática do esquecimento e da memória é a problemática essencial da proteção da vida privada. Não se trata de saber se a informação é confidencial ou pública, não é apenas isso: é também de saber se a produção da informação vai resistir ao tempo que passa. Nós podemos tomar o passado em plena face, sem que haja a profundidade do tempo que passa na restituição do que recebemos das redes e do que elas sabem sobre nós. Hoje, os motores de busca não avaliam a indexação de uma informação e sua restituição com base na temporalidade, mas de acordo com a relevância e popularidade em que não há escala de tempo. A relação com o tempo, que era previamente fixada pelo tempo de nossas vidas, deve mudar completamente."

A web realiza a expansão do ideal panóptico de controle pela intensa visibilidade. Esse mecanismo tem no sujeito o ponto de partida, mas não necessariamente o ponto de chegada, visto que fica a cargo das ferramentas interoperáveis, o registro geolocalizado de nossos rastros na web e nos espaços geográficos e os apontamentos informacionais fornecidos voluntariamente por nosso círculo íntimo contribuir para a consolidação de um perfil composto por diferentes camadas de informações que se articulam à revelia dos sujeitos.

Nesse contexto, é inegável que os recentes debates a respeito das mudanças sociotécnicas, os desdobramentos econômicos e os ordenamentos jurídicos provocaram rupturas inquietantes em relação aos objetos e aos princípios ordenadores do campo científico.

A abertura proporcionada pela Comissão Europeia (CNIL) acerca do direito ao esquecimento alterou radicalmente a regulação sobre a informação pessoal e consequentemente suas formas de tratamento e governança.

Concepção originalmente proposta GONZÁLEZ DE GOMÉZ (2002, p.35), a governança informacional

> "baseia-se na convergência teórico-conceitual da governança, accountability, transparência e do reconhecimento do direito e acesso à informação. Dessa forma, entende-se que a sustentação da formulação sobre a governança informacional reside na ciência política, na administração pública e comunicação pública e social. A ciência da informação contribui nessa formulação ao compreender a informação permeando e mediando as relações individuais e sociais, possibilitando com isso, a ampliação das bases comunicacionais do Estado com a sociedade civil, através do processo comunicativo dialógico." (RIBEIRO e ANDRADE, 2005, p.7)

O direito ao esquecimento é a garantia jurídica de supressão de dados pessoais disponíveis na web, tais como informações sensíveis "individuais" (questões políticas e econômicas, dados médicos, religião, sexualidade) e dados individuais (perfil de compra, circulação geográfica, imagens, dentre outras).

Esse instrumento legal, já aplicado na Europa desde 2014, representa um problema para os serviços de Inteligência de Estado, para a história e a memória social.

Do ponto de vista jurídico o respeito e a proteção dos dados pessoais, a intimidade e o direito ao esquecimento na Web ainda é subordinado ao entendimento sociopolítico da informação nos diferentes Estados nacionais, e se não há uma legislação clara, a pilhagem transnacional tem guarida.

De acordo com DONEDA (2014, p.143) o debate referente à proteção de dados pessoais se realiza há quatro décadas e se caracteriza por diferentes gerações de leis.

Na primeira geração tomou como referência a concessão de autorizações para a criação de bancos de dados e o seu controle por órgãos públicos. A segunda geração concentrou-se na constatação inevitável do caráter transnacional dos bancos de dados informatizados, todavia a proteção e a salvaguarda dos dados pessoais eram individualizadas. Na terceira geração de leis incorporou-se o exercício da autodeterminação informativa e buscou-se contemplar elementos que garantissem a autonomia do indivíduo em fornecer ou não o acesso aos seus dados pessoais.

A grande maioria das leis de proteção de dados pessoais foi criada na primeira década do século XXI e, conforme aponta GREENLEAF (2013), a lei

> "não é satisfeita por um código de conduta voluntário ou um esquema de certificação. A lei deve definir os princípios de privacidade de dados de uma forma específica, não

só como um princípio constitucional geral de proteção da privacidade, ou uma ação civil (responsabilidade civil) por violação de privacidade." (GREENLEAF,2013, p. 5),

Grande parte das leis de proteção de dados criada previa a constituição de uma Autoridade de Proteção de Dados (DPA) [4]. Além disso, foi pactuada uma série de princípios comuns relativos à formulação de normativas sobre a proteção de dados denominada "Fair Information Principles (FIPs). Os FIPs foram baseados no Guia de Privacidade da OCDE[5] de 1981 e na convenção nº. 108 de proteção dos dados, proposta pelo Conselho da Europa (CoE).

De acordo com DONEDA (2014, p. 146-150) a síntese de tais princípios envolve os seguintes elementos: transparência, qualidade, finalidade, livre acesso e segurança física e lógica.

Tab.1 - Núcleo comum das normativas sobre proteção de dados pessoais

Princípio	Escopo
Transparência	O tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados.
Qualidade	Os dados armazenados devem ser fiéis à realidade, atualizados, completos e relevantes. A coleta de dados deve ser feita com cuidado e correção e com atualizações periódicas.
Finalidade	Qualquer utilização de dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta dos mesmos. Estabelece-se por esse princípio a restrição no uso do dado pessoal e em sua transferência a terceiros.
Livre Acesso	O indivíduo deve ter livre acesso às suas informações armazenadas em bancos de dados, podendo obter cópias dos registros.
Segurança física e lógica	Os dados devem ser protegidos por meios técnicos e administrativos adequados contra o risco de extravio, destruição, modificação, transmissão ou acesso não autorizado.

Fonte: Adaptada de Doneda (2014) e Greenleaf (2013)

Da perspectiva de GREENLEAF (2012, p. 26) houve uma visível expansão da implementação de leis de proteção de dados pessoais no mundo inteiro nos últimos anos. Para o autor, as leis em vigor incorporaram pelo menos um conjunto mínimo de princípios de proteção de dados propostos pela OCDE e pelo Conselho da Europa, o que garante elementos fundamentais para o diálogo sobre essa matéria em âmbito internacional.

Todavia, é imprescindível considerar nesse quadro o avanço do desenvolvimento de tecnologias e práticas comerciais contrárias à privacidade de dados, em uma dinâmica de extrema valorização das informações pessoais. Desse ponto de vista, a implementação de leis de proteção não garantem, por si, a aplicação e a salvaguarda destas informações. Assim, o fortalecimento e institucionalização dessas leis requer a presença de organismos nacionais e internacionais que contribuam para a ampliação de sua aplicação, estabeleçam o seu monitoramento e fortaleçam as experiências locais.

3 A atividade de inteligência no contexto brasileiro

A atividade de inteligência é uma ação especializada e fundamentalmente informacional que envolve, conforme salienta GONÇALVES (2011: p. 7-8), produtos, organização e processos que visam apoiar o processo decisório. Suas ações têm como

[4] Data Protection Authority.
[5] Organização para a Cooperação Econômica e o Desenvolvimento.

foco o desenvolvimento de métodos e procedimentos que auxiliem na obtenção do dado negado.

Como produto revela a produção do conhecimento derivada de uma metodologia de inteligência. Como organização, refere-se às estruturas funcionais que objetivam a obtenção e a produção de conhecimentos de inteligência. Como atividade ou processo, refere-se aos procedimentos de obtenção de dados para a consecução da atividade de assessoramento ao processo decisório.

A atividade de inteligência trabalha principalmente com informações sensíveis e sigilosas e, quando desenvolvidas sob a denominação de inteligência de Estado, visa salvaguardar os interesses nacionais.

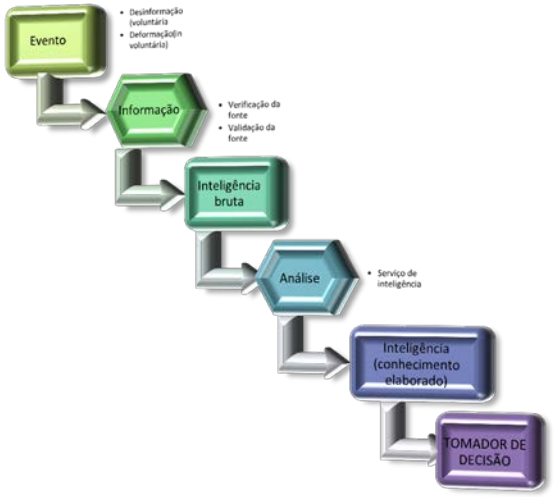
Conforme salienta OLIVEIRA (2013:p.11),

> "a inteligência é uma atividade correlata às Ciências Sociais que busca explicar, estimar e predizer eventos. Para tanto, dados e informações são coletados e analisados em um processo sistemático e contínuo cujo resultado é um produto informacional de elevado valor agregado."

No Brasil a atividade é regulada pela lei n. 9.833, de 07 de dezembro de 1999. Essa lei institucionalizou o Sistema Brasileiro de Inteligência (SISBIN) e criou a Agência Brasileira de Inteligência. A referida lei foi regulamentada pelo decreto n. 4.376 de 13 de setembro de 2002.

De acordo com GONÇALVES (2011: p. 115) a comunidade de inteligência no Brasil toma como fundamentos de suas ações a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana.

Fig. 1 – Do evento à inteligência



FONTE: GONÇALVES, Joanisval Brito.(2011) Atividade de inteligência e legislação correlata.

Embora sejam bastante inter-relacionadas a informação e a atividade de inteligência não devem ser justapostas, pois a inteligência incorpora o conhecimento sistematizado e a interpretação dirigida ao contexto.

A atividade de inteligência se organiza em: inteligência militar e de defesa, inteligência policial ou criminal e inteligência de segurança pública, inteligência financeira, inteligência competitiva, inteligência estratégica e inteligência de Estado.

Na condução das atividades, produtos e serviços, a atividade de inteligência adota os seguintes princípios norteadores: objetividade, oportunidade, segurança, imparcialidade, controle, clareza, simplicidade, amplitude e ética.

O princípio da objetividade refere-se à utilidade e finalidade das operações em relação ao propósito da operação. O princípio de oportunidade assinala que as informações produzidas com o propósito de subsidia uma atividade de inteligência

devem compreender agilidade e difusão aos atores envolvidos no processo. A segurança pauta-se pela natureza sigilosa da atividade e, nesse sentido, envolve apenas os atores que precisam saber da informação em construção ou processamento; desse ponto de vista, a informação é segmentada. A imparcialidade preconiza a isenção com que as informações devem ser produzidas e disseminadas pelos atores sociais implicados ao longo de uma atividade de inteligência. O controle ordena o escalão de informações e a centralização das atividades tendo como propósito orientar a ordem de produção e de difusão do conhecimento decorrente da atividade. A clareza refere-se à desejável compreensão da informação tratada e produzida no âmbito da atividade visando a sua rápida integração no processo de tomada de decisão. A simplicidade enfatiza que o produto da inteligência deve pauta-se pela apresentação de conhecimentos considerados essenciais na etapa em que serão utilizados. A amplitude enfatiza que os conhecimentos gerados devem ser amplos e exatos, porém sem se confrontar com os demais princípios relacionados à atividade. A ética é, nesse contexto, um princípio transversal que conduz toda a atividade de inteligência e preconiza a necessidade da ação pautar-se pelos princípios legais e constitucionais, tendo como foco o regime democrático em que a ação se realiza.

Em que pese o fundamento normativo da atividade de inteligência, a mesma é constantemente colocada sob suspeição pela sociedade civil, sobretudo naqueles países que passaram por ciclos recentes de regime militar, como é o caso do Brasil. A desconfiança se deve, principalmente, ao alto grau de autonomia, poder e capacidade operacional exercidas por esses serviços no âmbito dos Estados Nacionais.

O contexto internacional de fluxos de informação evidencia também uma tensão permanente em relação a tais atividades devido, sobretudo, ao grau de opacidade e conectividade das informações institucionais e pessoais que trafegam nos ambientes digitais abertos e/ou monitorados.

Os principais provedores dos dados e informações utilizados em atividades de inteligência são as fontes humanas, a inteligência técnica e as fontes abertas.

As fontes humanas correspondem a uma metodologia clássica de obtenção de informações. A adoção desse dispositivo implica no desenvolvimento de ações oficiais ou não oficiais para a coleta das informações. Nesse sentido, a informação utilizada pode ser obtida por espionagem deliberada ou por intermédio de agentes externos, sem um vínculo formal com a atividade.

A inteligência técnica ou tecnológica refere-se ao uso de dispositivos técnicos e ou tecnológicos para a coleta, sistematização e processamento da informação.

As fontes abertas, especialmente por se apresentarem em grande número devido aos processos globais de digitalização e disponibilização em rede, integram massivamente as atividades de inteligência. Dentre as principais fontes abertas estão: as mídias, os dados públicos e as informações profissionais e acadêmicas. Todavia, constata-se que a área de atividades de inteligência ainda é carente de procedimentos de análise e produção da informação que possam prover de inteligibilidades os dados que pervagam a web na atualidade.

4 A proteção de dados pessoais e o direito ao esquecimento digital no Brasil

A discussão sobre o direito ao esquecimento digital e à proteção de dados pessoais no Brasil é recente, se consideramos a história de criação de dispositivos legais em diferentes países.

Conforme ressalta DONEDA (2014, p.136), estamos vivendo um momento de redução do encantamento em relação às tecnologias. Trata-se de uma etapa de "cobrança da fatura" em que se acentuam as relações políticas e econômicas pautadas pela primazia no acesso à informação pessoal em ambientes digitais.

Em maio de 2007, o pesquisador Ronaldo Lemos já assinalava a necessidade de o Brasil estabelecer um marco civil para regulação da Internet no país, em oposição ao caráter criminal pretendido na ocasião. Segundo LEMOS (2007),

> "o caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é primeiramente estabelecer um marco regulatório civil, que defina

claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições acessando a rede, para a partir daí definir regras criminais.[6]".

Em seu artigo, LEMOS alertava para os efeitos penais que a equiparação entre "coisa" e dado ou informação poderia trazer no âmbito da legislação.

> "a Internet conta com características de várias mídias, muitas das quais representam comunicações efêmeras ou transitórias. Nesse sentido, uma "conversa telefônica" mantida pela Internet por meio de um programa como o Skype estaria sendo equiparada à "coisa" para fins penais. O mesmo é válido para conversas por texto, vídeos, fluxos de webcams, e-mails, bem como qualquer outra forma de comunicação. Essa equiparação à "coisa" sujeita os provedores a medidas judiciais que levem à possibilidade de reconstituição dessas informações transitórias, que podem então ser "apreendidas" e utilizadas em juízo. Isso desrespeita direitos e expectativas básicos com relação à natureza dos dados eletrônicos. "[7]

Em março de 2013, juristas brasileiros reunidos na 6ª. Jornada de Direito Civil do Conselho da Justiça Federal aprovaram o enunciado 531, em que reconhecem que "a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento."

O enunciado não é considerado obrigatório na interpretação do código civil brasileiro, todavia, acredita-se que o entendimento nele exposto pode nortear as decisões judiciais em relação aos litígios concernentes à perenidade da informação pessoal *online*, que uma vez regularizada, ainda possa causar constrangimentos à pessoa citada no ambiente digital.

Os juristas justificam que,

> "Os danos provocados pelas novas tecnologias da informação veem se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como uma parcela do direito do ex-detento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegurar a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados."[8]

Em outubro de 2013, algumas autoridades brasileiras, dentre elas a presidente da república, Dilma Rousseff, foram monitoradas pela Agência Nacional dos Estados Unidos (NSA), conforme denúncia do agente de inteligência estadunidense e atualmente exilado na Rússia, Edward Joseph Snowden. Na prática, o NSA coletou milhões de e-mails e analisou parte das informações oriundas das autoridades identificando fluxos de interações em diferentes meios de comunicação digital.

A grande perplexidade e repercussão social desse fato pode ter contribuído para a agilidade em sancionar o Marco Civil da Internet no Brasil, que, embora não verse exclusivamente sobre a proteção dos dados pessoais, assegura no artigo 10 que, "a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas".

A lei nº. 12.965 de 23 de abril de 2014, conhecida como "Marco Civil da Internet", é fruto de intensos debates no Brasil. O dispositivo legal "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria". A lei se fundamenta na liberdade de expressão e reconhece a escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a

---

[6] LEMOS, Ronaldo. Internet brasileira precisa de marco regulatório civil. 22/05/207. Disponível em: http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm

[7] IDEM

[8] Jornada de Direito Civil (6). Enunciados aprovados na VI Jornada de direito civil. Disponível em: http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/vijornada.pdf. Acesso em 10. Set. 2014.

colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; e a finalidade social da rede.

No que se refere à proteção de dados no Brasil, encontra-se em tramitação na Câmara dos Deputados o projeto de Lei 4.060/2012. O projeto de lei aguarda o parecer do Relator na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) e tem por objetivo "garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem".

As leis de proteção de dados pessoais almejam em última instância salvaguardar a pessoa. Nesse aspecto DONEDA (2014, p.147) ressalta que uma consequência natural de uma lei futura no Brasil será a limitação das possibilidades de o Estado e as empresas utilizarem livremente os dados pessoais que estão sob a sua tutela e isso levará a uma série de adaptações de ordem cultural e política. O autor destaca que,

> "A confirmação do cidadão com o único sujeito que pode, legitimamente, tomar decisões sobre a modalidade de tratamento de seus próprios dados pessoais, juntamente com a instituição de instrumentos de monitoramento e de tutela capazes de coibir, efetivamente, os tratamentos abusivos de dados pessoais, consolida as bases para que o direito à privacidade e a proteção de dados pessoais seja percebida como um aspecto essencial da liberdade contemporânea." (DONEDA, 2014: P.147).

Pode se afirmar que atualmente experimenta-se no Brasil uma "virada informacional" em que aspectos cruciais do direito à informação, salvaguarda da intimidade e a restituição da verdade são colocados na ordem do dia, em um país que viveu sob a égide do cerceamento informacional decorrente de um longo período ditatorial. Compreender a importância histórica e social desse momento é imprescindível para se pensar em uma sociedade da informação pautada pelo respeito aos fluxos informacionais produzidos, preservados e transacionados em diferentes instâncias.

5 Considerações finais

A formação humana em Ciência da Informação tem sido particularmente tensionada nos últimos anos. Percebe-se que os novos modelos de negócio pactuados em rede, os conflitos de interesses entre os Estados Nacionais, os indícios de guerras informacionais, a popularização dos dispositivos de vigilância, hoje vendidos em papelarias, bem como as novas dimensões conceituais e técnicas da governança informacional requerem uma reflexão mais detida do campo.

Nesse trabalho, buscou-se articular duas dimensões que tradicionalmente são marcadas por antagonismos e tratadas separadamente: as atividades de inteligência e a salvaguarda dos dados pessoais. Buscou-se também tornar evidente que, por razões políticas, econômicas, sociais e tecnológicas, esses elementos incidem objetivamente no campo da Ciência da Informação devido fato de o campo responsabilizar-se tecnicamente pelos processos de governança informacional nos diversos contextos. Enfatizou-se que a aparente neutralidade técnica adotada no campo revela um risco de atuação profissional demarcada por um alheamento político.

Nesse sentido, constata-se que uma atenção e envolvimento das instituições voltadas à pesquisa e à formação humana na ampliação da agenda, em relação a esse contexto, são desejáveis e urgentes.

Acredita-se que pensar a governança informacional para além do fluxo ordenado de informações e dados requer forçosamente incluir a formação humana como uma dimensão importante à soberania e autodeterminação informativa dos Estados Nacionais. Desse ponto de vista, o campo da Ciência da Informação e os profissionais a ele associados são parte imprescindível nesse debate.

6 Agradecimentos

Agradecimentos são devidos à Fundação de Amparo à Pesquisa de Minas Gerais (FAPEMIG), ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)

e à Associação Internacional para Estudos de Segurança e Inteligência – INASIS pelo apoio dado ao desenvolvimento desse trabalho.

7 Referências

Agence des Droits Fondamentaux de L'union Européenne. Manuel de droit européen en matière de protection des données. (2014). Disponível em: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_fr.pdf. Acesso em 29 jun.2014.

Averna, Louise, Beaufond, Christelle Huyghue (2013). Le droit à l' oubli numérique. Paris: Université Paris Ouest. http://www.e-juristes.org/wp-content/uploads//2014/03/le-droit-%C3%A0-loubli-num%C3%A9rique-finale.pdf Acesso em 30. jul.2015.

Bauman, Zygmunt (2013). *Vigilância líquida*. Rio de Janeiro: Zahar.

Brasil. Lei nº. 12.965, de 23 abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em 13 set. 2015.

Brasil. Projeto de Lei 4.060/2012. Proteção de Dados Pessoais. Dispõe sobre a proteção de dados pessoais, a privacidade e dá outras providências. Disponível em: ‹http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066›. Acesso em: 10. set. 2015.

Direito ao esquecimento é debatido por juristas e especialistas. Disponível em: ‹http://www.ebc.com.br/noticias/brasil/2014/06/direito-ao-esquecimento-e-debatido-por-juristas-e-especialistas.› Acesso 29 ago 2015.

Doneda, Danilo (2014). A proteção da privacidade e de dados pessoais no Brasil. *Observatório Itaú Cultural*, v. 16, p.136-150, jan./jun.2014.

Estienne, Yannick Un monde de verre: Facebook ou les paradoxes de la vie privée (sur)exposée. Disponível em: ‹http://www.lecreis.org/colloques%20creis/2010/Communication-Estienne-CREIS.pdf.› Acesso em: 31 jan. 2014.

Foucault, Michel (2008). Segurança, Território, População. Curso dado no Collège de France (1977-1978). Trad. Eduardo Brandão. São Paulo: Martins Fontes, 2008.

González de Gómez, Maria Nélida (2002). Novos cenários políticos para a informação. Ciência da Informação. Brasília, v.31, n.1, p. 27-40, jan./abr.

Jornada de direito civil (6, Brasília, junho 2013). Enunciados aprovados na VI Jornada de direito civil. Disponível em: ‹http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/vijornada.pdf.› Acesso em 10 set 2015.

Gonçalves, Joanisval Brito (2011). Atividade de inteligência e legislação correlata. Niterói: Ed. Impetus.

Greenleaf, Graham (2013). Sheherezade and the 101 data privacy laws: origins, significance and global trajectories. Journal of Law, Information & Science, Sep., v.23, n. 1. Disponível em ‹http://ssrn.com/abstract=2280877 ›

Kaltenbach, Laure, Le Guay, Olivier (2013). Pour l'intimité numérique des droits universels pour protéger notre identité 2.0. Paris, Le Monde. 22. nov.

Lima, C. C. C.; Monteiro, R. L. (2013). Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. AtoZ: novas práticas em informação e conhecimento, Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: ‹http://www.atoz.ufpr.br›. Acesso em: 29. jun. 2014.

Lemos Ronaldo. Internet brasileira precisa de marco regulatório civil. 22/05/2007. Disponível em: http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm. Acesso em 15. Jul. 2014.

Olivera, Henrique Figueiredo Machado de (2013). Reflexões sobre o conceito de inteligência. *Revista Brasileira de Ciências Policiais*. Brasília, v. 4, n. 2, p. 11-23, jul/dez 2013.

Orwell, George (2009). *1984*. São Paulo: Companhia das Letras.

Tribunal de Justiça da União Europeia. Comunicado de imprensa n° 70/14. Acórdão no processo C-131/12 Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070pt.pdf. Acesso em 14 set. 2014.

Ribeiro, Carla Andrea, Andrade, Maria Eugênia Albino. Governança informacional como sustentação das ações de combate à corrupção. XVIII Concurso del CLAD sobre Reforma del Estado y Modernización de la Administración Pública "Cómo combatir la corrupción, garantizar la transparencia y rescatar la ética en la

gestión gubernamental en Iberoamérica". Caracas, 2004-2005. 49 p. Disponível em ‹http://siare.clad.org/fulltext/0052001.pdf›. Acesso em 5. Out.2014.

Santos, Rone Eleandro dos (2010). *Genealogia da Governamentalidade em Michel Foucault*. Belo Horizonte: FAFICH/UFMG, 2010. 242 p.